

### REMARKS

In view of the above amendments and the following remarks, reconsideration and further examination are respectfully requested.

Initially, the Applicant would like to thank Examiner William Treat for granting and conducting a telephone interview on February 20, 2008 in connection with the above-identified application.

The specification and abstract have been reviewed and revised to improve their English grammar. The amendments to the specification and abstract have been incorporated into a substitute specification and abstract. Attached are two versions of the substitute specification and abstract, a marked-up version showing the revisions, as well as a clean version. No new matter has been added.

Independent claims 1, 18 and 19 have been amended, and claims 2-5, 7-9, 14, 16 and 20-22 have been cancelled to address the Examiner's rejections.

Further, claims 1, 6, 10-13, 15, and 17-19 have been amended to make a number of editorial revisions thereto. These editorial revisions have been made to place the claims in better U.S. form. Further, these editorial revisions have not been made to narrow the scope of protection of the claims, or to address issues related to patentability, and therefore, these amendments should not be construed as limiting the scope of equivalents of the claimed features offered by the Doctrine of Equivalents.

Claims 1-22 were rejected under 35 U.S.C. § 112, second paragraph, for being incomplete for omitting essential elements and/or steps and for failing to enable a person of ordinary skill in the art to make and/or use the claimed invention.

As discussed during the above-mentioned telephone interview, independent claims 1, 18, and 19 have been amended to define a specific order to the mathematical operations (i.e., first generating elements belonging to a group G, second generating an operation value, etc.). Further, claims 1, 18, and 19 have been amended to include specific mathematical operations so that a person of ordinary skill in the art would be able to make and/or use the claimed invention.

Therefore, this rejection is believed clearly inapplicable to amended independent claims 1, 18, and 19 and the claims that depend therefrom, since, as discussed above, claims 1, 18, and

19 have been amended to specifically avoid the problems identified by the Examiner and to otherwise comply with the requirements of 35 U.S.C. § 112, second paragraph. Thus, withdrawal of this rejection is respectfully requested.

Claims 19-22 were rejected under 35 U.S.C. § 101 for reciting a computer program, which is non-statutory subject matter. Claim 19 has been amended to recite a computer-readable storage medium having a computer program stored thereon. Further, claims 20-22 have been cancelled. Therefore, since claim 19 now recites statutory subject matter, withdrawal of this rejection is respectfully requested.

Claims 1-13 and 17-22 were rejected under 35 U.S.C. § 101 for merely claiming a mathematical algorithm without setting forth a practical application for the algorithm.

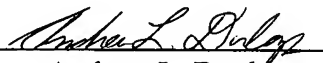
As discussed during the above-mentioned telephone interview, independent claims 1, 18, and 19 have been amended to include recitations directed to the “security processing,” as recited in original dependent claims 2, 14, and 16. It is noted that the “securing processing,” now recited in claims 1, 18, and 19, includes limitations which provide a concrete and practical application for the algorithm recited in the independent claims.

Therefore, because independent claims 1, 18, and 19 now recite patentable subject matter, it is respectfully submitted that this 35 U.S.C. § 101 rejection is inapplicable to claims 1, 18, and 19, and claims 6, 10-13, 15, and 17 which depend therefrom. Thus, withdrawal of this rejection is respectfully requested.

In view of the above amendments and remarks, it is submitted that the present application is now in condition for allowance and an early notification thereof is earnestly requested. The Examiner is invited to contact the undersigned by telephone to resolve any remaining issues.

Respectfully submitted,

Yuichi FUTA et al.

By:   
Andrew L. Dunlap  
Registration No. 60,554  
Attorney for Applicants

ALD/led  
Washington, D.C. 20006-1021  
Telephone (202) 721-8200  
Facsimile (202) 721-8250  
March 18, 2008